ASA: Receiving and Transmitting Jumbo Ethernet Frames

Contents

Introduction

This document provides information how the Adaptive Security Appliance (ASA) receives and transmits jumbo ethernet frames.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Jumbo frame support on the ASA

Enabling jumbo frame support requires specific Adaptive Security Appliance (ASA) hardware and software versions, as well as a reboot. For more information on the supported models and versions, as well as how to enable jumbo frames, refer to the ASA 8.4 configuration guide section, Enabling Jumbo Frame Support (Supported Models).

Note that after enabling jumbo frame support and rebooting the ASA, these additional actions should be taken to make full use of jumbo frames:

- The MTU of the ASA interfaces must be increased with the **mtu** command in interface sub-configuration mode so that the ASA will transmit jumbo frames.
- The ASA must be configured to adjust the TCP MSS for TCP connections to a higher value than the default. If this is not done, ethernet frames containing TCP data will not be larger than 1500 bytes. The TCP MSS should be adjusted to 120 bytes less than the lowest setting for the interface MTU. If the interface MTU is 9216, then the MSS should be configured to 9096. This can be done with the **sysopt connection tcpmss** command.

What if the ASA is not configured for jumbo frames and it receives a jumbo frame?

The **jumbo frame-reservation** command allows not only the transmission of jumbos, but also the reception. Without jumbo frame support enabled, the ASA will drop packets that are too large. These drops are counted under the "giant" statistic in the **show interface** output:

```
ASA# show interface Interface GigabitEthernet0/0 "inside", is up, line protocol is up
Hardware is bcm56801 rev 01, BW 1000 Mbps, DLY 10 usec Auto-Duplex(Full-duplex),
Auto-Speed(1000 Mbps) Input flow control is unsupported, output flow control is on
MAC address 5475.d029.8916, MTU 1500 IP address 10.36.29.1, subnet mask 255.255.0.0
499 packets input, 52146 bytes, 0 no buffer Received 63 broadcasts, 0 runts, 5 giants
<---- HERE
```

What if the ASA successfully receives a jumbo frame but attempts to send it out an interface with a lower MTU?

In order to receive a jumbo frame, the ASA must have the jumbo-frame reservation command, but does not necessarily need to have the MTU increased (because that only affects the maximum transmission size for the interface, not the reception).

If the ASA successfully receives a jumbo frame, but that frame is then too large to transmit out the egress interface, these situations can occur depending on the setting of the Don't Fragment (DF) bit in the IP header of the packet:

- If the DF bit is set in the IP header, the ASA will drop the packet and send a ICMP type 3 code 4 message back to the sender.
- If the DF bit is not set, the ASA will fragment the packet and transmit the fragments out the egress interface.

This is an ASA CLI session that utilizes packet captures to show the ASA receiving a jumbo frame on the inside interface (with a size of 4014 bytes) that is too large to transmit out egress interface (the outside has a MTU of 1500). **In this case the DF bit is not set in the IP header**. The packet is fragmented on egress out the outside interface:

```
ASA# show cap in detail 20 packets captured 1: 11:30:30.308913 0017.0f17.af80
5475.d029.8916 0x0800 4014: 10.99.103.6 > 10.23.124.1: icmp: echo request (ttl 255,
id 48872) 2: 11:30:30.309920 5475.d029.8916 0017.0f17.af80 0x0800 1514: 10.23.124.1 >
10.99.103.6: icmp: echo reply (wrong icmp csum) (frag 48872:1480@0+) (ttl 255) 3:
11:30:30.309935 5475.d029.8916 0017.0f17.af80 0x0800 1514: 10.23.124.1 > 10.99.103.6:
(frag 48872:1480@1480+) (ttl 255) 4: 11:30:30.309935 5475.d029.8916 0017.0f17.af80
```

```
0x0800 1054: 10.23.124.1 > 10.99.103.6: (frag 48872:1020@2960) (ttl 255) ... ASA#
show cap out detail 30 packets captured 1: 11:30:30.309035 5475.d029.8917
001a.a185.847f 0x0800 1514: 10.23.124.142 > 10.23.124.1: icmp: echo request (wrong
icmp csum) (frag 48872:1480@0+) (ttl 255) 2: 11:30:30.309035 5475.d029.8917
001a.a185.847f 0x0800 1514: 10.23.124.142 > 10.23.124.1: (frag 48872:1480@1480+) (ttl
255) 3: 11:30:30.309050 5475.d029.8917 001a.a185.847f 0x0800 1054: 10.23.124.142 >
10.23.124.1: (frag 48872:1020@2960) (ttl 255) 4: 11:30:30.309859 001a.a185.847f
5475.d029.8917 0x0800 1514: 10.23.124.1 > 10.23.124.142: icmp: echo reply (wrong icmp
csum) (frag 48872:1480@0+) (ttl 255) 5: 11:30:30.309859 001a.a185.847f 5475.d029.8917
0x0800 1514: 10.23.124.1 > 10.23.124.142: (frag 48872:1480@1480+) (ttl 255) 6:
11:30:30.309859 001a.a185.847f 5475.d029.8917 0x0800 1054: 10.23.124.1 >
10.23.124.142: (frag 48872:1020@2960) (ttl 255)
```

This is an example showing an ASA receiving a jumbo frame on the inside interface too large to transmit out the egress interface, **and the packet has the DF bit set**. The packet is dropped and the ICMP type 3 code 4 error message is transmitted towards the inside host:

```
ASA# show cap in detail 6 packets captured 1: 11:42:10.147422 0017.0f17.af80
5475.d029.8916 0x0800 4014: 10.99.103.6 > 10.23.124.1: icmp: echo request (DF) (ttl
255, id 48887) 2: 11:42:10.147605 5475.d029.8916 0017.0f17.af80 0x0800 70: 10.99.29.1
> 10.99.103.6: icmp: 10.23.124.1 unreachable - need to frag (mtu 1500) (ttl 72, id
56194) 3: 11:42:10.150199 0017.0f17.af80 5475.d029.8916 0x0800 4014: 10.99.103.6 >
10.23.124.1: icmp: echo request (DF) (ttl 255, id 48888) 4: 11:42:12.146476
0017.0f17.af80 5475.d029.8916 0x0800 4014: 10.99.103.6 > 10.23.124.1: icmp: echo
request (DF) (ttl 255, id 48889) 5: 11:42:12.146553 5475.d029.8916 0017.0f17.af80
0x0800 70: 10.99.29.1 > 10.99.103.6: icmp: 10.23.124.1 unreachable - need to frag
(mtu 1500) (ttl 72, id 45247) 6: 11:42:12.152427 0017.0f17.af80 5475.d029.8916 0x0800
4014: 10.99.103.6 > 10.23.124.1: icmp: echo request (DF) (ttl 255, id 48890) 6
packets shown ASA# show cap out detail 0 packet captured 0 packet shown ASA#
```

Related Information

- **Technical Support & Documentation - Cisco Systems**